UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,665	02/02/2001	Donald B. Johnson	6944-8-1	7060

293 7590 12/20/2004

Ralph A. Dowell of DOWELL & DOWELL P.C.
2111 Eisenhower Ave.
Suite 406
Alexandria, VA 22314

EXAMINER	
KLIMACH, PAULA W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 12/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/773,665	JOHNSON ET AL.	
	Examiner	Art Unit	
	Paula W Klimach	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 July 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02/02/2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Double Patenting

A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

Claims 1-9 are rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1-9 of prior U.S. Patent No. 6, 279, 110. This is a double patenting rejection.

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 10-11 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 10-11 of U.S. Patent No. 6,279,110. Although the conflicting claims are not identical, they are not patentably distinct from each other because the application claims a means for generating (claim 10 lines 6-8), while the patent '110

discloses a generator (claim 10 lines 7-9). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a generator as disclosed in '110 as a means for generating. One of ordinary skill in the art would have been motivated to do this because this is the function of a generator.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1 and 7 recite the limitation "said long term private key" in line 10 and 11 respectively. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia (5, 825,880) in view of Koyama et al.

In reference to claims 1, 7, and 10, Sudia discloses a signing system and method to affix a signature using multiple partial signatures (abstract) comprising steps of: generating a first short term private key; computing a first short term public key derived from said first short term private key (column 11 lines 1-5 in combination with column 11 lines 24-26). Sudia discloses

the calculation of several partial signatures (signature components) and finding the normal signature using the multiplicative properties of digital signatures (column 5 lines 1-37). Finally Sudia discloses a system that receives the signature and verifies said signature (column 3 lines 21-30).

However Sudia does not disclose computing the signature component using the public key.

Koyama teaches creating of a partial signature using the public key. Koyama further teaches combining partial signatures using homomorphism and a masked digital signature (section 7.4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use homomorphism to calculate a digital signature as in Koyama in the system of Sudia. One of ordinary skill in the art would have been motivated to do this because calculating the digital signature as in Koyama uses elliptic curve, which provides method of calculating the digital signature in a method that is less computationally expensive and the algorithms are analogues to RSA algorithms.

In reference to claim 2, wherein said first short term private key k is an integer and said first short term public key is derived by computing the value kP = (x1, y1) wherein P is a point of prime order n in E(Fq), wherein E is an elliptic curve defined over Fq.

Sudia does not disclose a system that uses elliptic curve.

Koyama discloses a system to compute signatures wherein private and public key are derived by computing the value kP = (x1, y1) wherein P is a point of prime order n in E(Fq), wherein E is an elliptic curve defined over Fq (section 3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use homomorphism to calculate a digital signature as in Koyama in the system of Sudia. One of ordinary skill in the art would have been motivated to do this because calculating the digital signature as in Koyama uses elliptic curve, which provides method of calculating the digital signature in a method that is less computationally expensive and the algorithms are analogues to RSA algorithms.

In reference to claim 3, wherein said first signature component r having a form defined by r = x (mod n) wherein x is derived by converting said coordinate x1 to an integer x .

Sudia does not disclose a system that uses elliptic curve.

Koyama discloses a system wherein said first signature component r having a form defined by r = x (mod n) wherein x is derived by converting said coordinate x1 to an integer x (section 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use homomorphism to calculate a digital signature as in Koyama in the system of Sudia. One of ordinary skill in the art would have been motivated to do this because calculating the digital signature as in Koyama uses elliptic curve, which provides method of calculating the digital signature in a method that is less computationally expensive and the algorithms are analogues to RSA algorithms.

In reference to claim 4, wherein said second short term private key being an integer selected such that 2 <= t <= (n-2), and said second signature component being defined by s = t (e + dr)(mod n), wherein e is a hash of said message m.

Sudia does not disclose a system that uses elliptic curve for calculating the second digital signature.

Koyama discloses a system wherein the key is an integer selected such that 2 <= t <= (n-2), and said second signature component being defined by s = t (e + dr)(mod n), wherein e is a hash of said message m (section 7.4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use homomorphism to calculate a digital signature as in Koyama in the system of Sudia. One of ordinary skill in the art would have been motivated to do this because calculating the digital signature as in Koyama uses elliptic curve, which provides method of calculating the digital signature in a method that is less computationally expensive and the algorithms are analogues to RSA algorithms.

In reference to claim 5, wherein the third signature component being defined by c = tk (mod n) .

Sudia does not disclose a system that uses elliptic curve for calculating the second digital signature.

Koyama discloses a system wherein the signature components being defined by c = tk (mod n) (section 7.4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use homomorphism to calculate a digital signature as in Koyama in the system of Sudia. One of ordinary skill in the art would have been motivated to do this because calculating the digital signature as in Koyama uses elliptic curve, which provides method of

calculating the digital signature in a method that is less computationally expensive and the algorithms are analogues to RSA algorithms.

In reference to claims 6 and 11 wherein said normal signature component s being defined by $s` = c^{-1}s \bmod n$.

Koyama discloses a system wherein said normal signature component s being defined by $s` = c^{-1}s \bmod n$ (section 7.4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use homomorphism to calculate a digital signature as in Koyama in the system of Sudia. One of ordinary skill in the art would have been motivated to do this because calculating the digital signature as in Koyama uses elliptic curve, which provides method of calculating the digital signature in a method that is less computationally expensive and the algorithms are analogues to RSA algorithms.

In reference to claims 8-9 that includes the step of in said receiver computer system, using said second and third signature components (s, r) computing a normal signature component s`, and sending said signature components (s`, r) as a normal digital signature to a verifier computer system, and verifying said normal signature (s, r) by said verifier system (column 5 lines 35-40).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Demytko 5,627,893

Boneh Twenty Years of Attacks on the RSA Cryptosystem

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK
Thursday, December 09, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100